

526 Rec'd PCT/PTO 12 JUN 2000

FORM PTO-1350  
(REV. 5-93)

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER  
10191/1452

**TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371**

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

**09/581459**

INTERNATIONAL APPLICATION NO.  
PCT/DE98/03431

INTERNATIONAL FILING DATE  
(20.11.98)  
20 November 1998

PRIORITY DATE CLAIMED:  
(11.12.97)  
21 December 1997

TITLE OF INVENTION

**SYSTEM FOR CONTROLLING ACCESS AUTHORIZATION**

APPLICANT(S) FOR DO/EO/US

**Stephan SCHMITZ and Hans-Joerg MATHONY**

Applicants herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
- ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
- ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
- ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
- ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
  - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☒ has been transmitted by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
- ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
- ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
  - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☐ have been transmitted by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) (unsigned).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report.

PCT/RO/101.

EXPRESS MAIL NO.: **21302699756**

NY01 289356

CALCULATIONS | PTO USE ONLY

17. ☒ The following fees are submitted:**Basic National Fee (37 CFR 1.492(a)(1)-(5)):**Search Report has been prepared by the EUROPEAN PATENT OFFICE or  
JPO ..... \$840.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) ..... \$670.00

No international preliminary examination fee paid to USPTO (37 CFR 1.482) but  
international search fee paid to USPTO (37 CFR 1.445(a)(2)) ..... \$750.00Neither international preliminary examination fee (37 CFR 1.482) nor international search  
fee (37 CFR 1.445(a)(2)) paid to USPTO ..... \$970.00International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims  
satisfied provisions of PCT Article 33(2)-(4) ..... \$96.00**ENTER APPROPRIATE BASIC FEE AMOUNT =**

\$840

Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months  
from the earliest claimed priority date (37 CFR 1.492(e)).

\$

Claims

Number Filed

Number Extra

Rate

Total Claims

9 - 20 =

0

X \$18.00

\$

Independent Claims

1 - 3 =

0

X \$78.00

\$ 0

Multiple dependent claim(s) (if applicable)

+ \$260.00

\$

**TOTAL OF ABOVE CALCULATIONS =**

\$ 840

Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must  
also be filed. (Note 37 CFR 1.9, 1.27, 1.28).

\$

**SUBTOTAL =**

\$ 840

Processing fee of \$130.00 for furnishing the English translation later the ☐ 20 ☐ 30  
months from the earliest claimed priority date (37 CFR 1.492(f)).

+

\$

**TOTAL NATIONAL FEE =**

\$ 840

Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be  
accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property

+

\$

**TOTAL FEES ENCLOSED =**

\$ 840

Amount to be:

refunded \$

charged \$

a. ☐ A check in the amount of \$ \_\_\_\_\_ to cover the above fees is enclosed.b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of \$840.00 to cover the above fees. A duplicate copy of this sheet  
is enclosed.c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit  
Account No. 11-0600. A duplicate copy of this sheet is enclosed.**NOTE:** Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be  
filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Kenyon &amp; Kenyon

One Broadway

New York, New York 10004

SIGNATURE

Richard L. Mayer, Reg. No. 22,490

NAME

DATE

09/581459

416 Rec'd PCT/PTO 12 JUN 2000

[10191/1452]

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant(s) : SCHMITZ et al.  
Serial No. : To Be Assigned  
Filed : Herewith  
For : SYSTEM FOR CONTROLLING  
ACCESS AUTHORIZATION  
Examiner : To Be Assigned  
Group Art Unit : To Be Assigned

Assistant Commissioner  
for Patents  
Washington, D.C. 20231

**PRELIMINARY AMENDMENT**

SIR:

Please amend the above-identified application before examination as follows:

**In The Specification:**

On page 1, line 1, change "Background Information" to --Background Information--.

On page 1, line 3, after "The" insert --present--.

On page 1, line 3, after "authorization" insert --,-- and delete "as set forth by".

On page 1, delete line 4 and insert --German Patent No. 44 28 947 has--.

On page 1, line 12, insert --Summary Of The Invention--.

81302699756

09/581459 07/27/00

On page 1, line 14, delete "The objective is achieved by the characterizing features of".

On page 1, delete line 15.

On page 1, line 21, before "invention" insert --present--.

On page 3, delete lines 11-23 and in their place insert:  
--Brief Description Of The Drawings

Figure 1 shows a block diagram and an access authorization procedure of a first exemplary embodiment.

Figure 2 shows another block diagram and access authorization procedure of the first exemplary embodiment.

Figure 3 shows a block diagram and an access authorization procedure of a second exemplary embodiment.

Figure 4 shows another block diagram and access authorization procedure of the second exemplary embodiment.

Detailed Description--.

On page 4, line 25, delete "it is essential that".

On page 4, line 26, change "be" to --is--.

On page 4, line 27, after "Rx," insert --and--.

On page 5, line 27, after "CWx," insert --and--.

09581459, 072700

On page 5, line 32, after "agree," insert --the procedure-- .

On page 6, line 1, after "then" insert --the procedure-- .

On page 6, line 6, change "must be" to --is--.

On page 7, line 1, change "Patent Claims" to  
--What Is Claimed Is--.

**In The Claims:**

Please cancel original claims 1-9, without prejudice, in the underlying PCT application, and also cancel the substitute claims 1-9, without prejudice, and enter the following new claims.

10. (New) A system for controlling an access authorization, comprising:  
a base device for receiving a code word containing a reply and including a computer for comparing the reply to a required reply, wherein an access is authorized if the reply and the required reply agree; and  
at least one remote control for transmitting the code word, wherein:  
the base device transmits a prompt signal within a framework of a prompt/reply that has been previously successfully carried out, and  
the prompt signal is stored in the at least one remote control.
11. (New) The system according to claim 10, wherein:  
the required reply is formed as a function of an identifier stored in the at least one remote control and contained in the code word.
12. (New) The system according to claim 10, wherein:  
the prompt signal is stored in the base device.

09581459.072700

13. (New) The system according to claim 12, wherein:  
the prompt signal stored in the base device is erased when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value.
14. (New) The system according to claim 10, wherein:  
the code word includes a counter code that is compared by the base device to a reference code.
15. (New) The system according to claim 14, wherein:  
the counter code is changed in response to an actuation of an operating control element of the at least one remote control.
16. (New) The system according to claim 14, wherein:  
the counter code is transmitted, and  
the transmitted counter code serves as the reference code.
17. (New) The system according to claim 14, wherein:  
the counter code is contained in encrypted form in the code word.
18. (New) The system according to claim 10, wherein:  
the code word is transmitted at a high frequency, and  
the prompt signal is transmitted at a low frequency.

**In The Abstract:**

Delete the Abstract and insert:

**--Abstract Of The Disclosure**

A system is proposed for controlling access authorization. It includes a base device which receives a code word that contains a response. A computer compares the response to a required response. An access is authorized if the response and the required response agree. A remote control transmits the code word. The system has

09584459.072700

the distinction that a challenge transmitted by the base device is stored in the remote control for generating the code word.--.

### Remarks

This Preliminary Amendment cancels original claims 1-9, without prejudice, in the underlying PCT Application No. PCT/DE98/03431, and cancels substitute claims 1-9, without prejudice. This Preliminary Amendment also adds new claims 10-18. The new claims do not add new matter to the application, but do conform the claims to U.S. Patent and Trademark Office rules.

The amendments to the specification and abstract are to conform the specification and abstract to U.S. Patent and Trademark Office rules. The amendments to the specification and abstract do not introduce new matter into the application.

The underlying PCT application includes a Search Report dated May 18, 1999, and an International Preliminary Examination Report dated November 18, 1999, copies of which are submitted herewith.

Applicants assert that the present invention is new, non-obvious, and useful. Consideration and allowance of the claims are requested.

Respectfully submitted,

KENYON & KENYON

By: *Richard L. Mayer* (Reg. No. 41,172)

Dated: 6/12/00

By: *Richard L. Mayer*  
Richard L. Mayer  
Reg. No. 22,490

One Broadway  
New York, NY 10004  
(212) 425-7200

SYSTEM FOR CONTROLLING ACCESS AUTHORIZATION

## Background Information

5 The invention is based on a system for controlling access authorization as set forth by the species defined in the independent claim. The German patent 44 28 947 C1 has already described a locking device for a motor vehicle having an actuating device as well as a transponder. Upon actuation of a transmitter, a remote-actuation changeable code word can be generated; a decoding device receives the code word, compares it to a remote-actuation changeable code signal stored in the decoding device, and generates an unlocking signal as a function of the comparison. Moreover, to increase security, a transponder is provided whose changeable code signal is also evaluated for an enablement.

The object of the present invention is to simplify the aforesaid system without suffering a loss in security. The objective is achieved by the characterizing features of the independent claim.

20 The system of the present invention for controlling access authorization includes a base device which receives a code word. The code word contains a response which a computer compares to a required response. An access is authorized if the response and the required response agree. At least one remote control transmits the code word. The system according to the invention has the distinction that a challenge transmitted by the base device is stored in the remote control for generating the code word. This challenge is identical to that of a challenge/response process already successfully implemented in the past. Thus, the challenge gives an indication of an authorization of the remote control. In this manner, possibilities for manipulation are restricted. On the other hand, a fresh bidirectional challenge/response process is no longer necessary for the start of an access authorization procedure, since the challenge is already stored in the memory of the remote control. In this way, the code word can already be



transmitted with a greater transmission range to the base device, while the challenge/response procedure can only be carried out at short distance. Thus, a decoupling between bidirectional data transmission and unidirectional data transmission is ensured. Only a transmitter of greater transmission range is to be provided in the remote control, but not a corresponding receiver for the remote area. The challenge can be used for synchronization between the base device and remote control. In addition, the response and the required response, respectively, directly decisive for the access authorization are not stored in either the base device or in the remote control, so that direct access to this security-relevant information is not possible.

In an expedient further development, the required response is formed as a function of an identifier stored in the remote control and contained in the code word. In this manner, an unequivocal allocation is achieved between the remote control used and the corresponding encryption stored in the base device. A clear allocation guarantees sufficiently high security against unauthorized manipulation attempts. Because of this, the algorithm which, in the remote control, encrypts the stored challenge - for example, using an identifier specific to the remote control - to form a response can simply be omitted and integrated in a microcontroller.

In one refinement, the challenge stored in the base device is erased after a predefined number of failed agreements of response and required response. This ensures that, given a number of failed opening attempts, an access is no longer authorized in response to further attempts. A renewed opening attempt is only to be permitted in conjunction with a successfully flowing challenge/response process. Upon failure of the access authorization via the unidirectional protocol, the security requirements are increased, in that an access can only be achieved in conjunction with the complex bidirectional protocol.

According to one advantageous refinement, the code word includes a counter code which the base device compares to a reference code. An access is only authorized in response to a deviation. The counter code is changed with the actuation of an operating control element of the remote control. Transmission of the code word just

monitored does not trigger an access authorization. The counter reading can be present both in unencrypted and in encrypted form in the code word.

A transmitted code is used as reference code. A separate counter function does not have to be provided in the base device for this purpose.

Expediently, the code word is transmitted at high frequency and the challenge is transmitted at low frequency. Because of the stored challenge, the remote control does not need a receiver in the high-frequency range.

Other useful further developments come to light from the description and from further dependent claims.

#### Drawing

Two possible exemplary embodiments of a system according to the present invention for controlling access authorization are shown in the drawing and are explained in greater detail in the following description. Figures 1 and 2 show a block diagram and an access authorization procedure of a first exemplary embodiment; Figures 3 and 4 show a block diagram and an access authorization procedure of a second exemplary embodiment.

#### Description

A plurality of remote controls F1, ... Fx, ... Fn communicate with a base device BG which includes a transmitter/receiver 12 and a computer 16. Computer 16 exchanges data with transmitter/receiver 12 and has access to challenges C1, ... Cx, ... Cn, identifiers K1, ... Kx, ... Kn and a limiting value G stored in the memory. The design of the xth remote control Fx is shown by way of example. A remote-control computer 20 has access to identifier Kx and challenge Cx stored in the memory. It supplies data to transmitter 22 and exchanges data with a remote-control transmitter/receiver 26. The signal state influenced by an operating control element 24 is supplied to remote-control computer 20.

The second exemplary embodiment according to Figure 3 differs from the first exemplary embodiment according to Figure 1 in that, instead of limiting value G, a memory for a reference code RZ1, ... RZx, ... RZn is provided in base device BG. Remote control Fx has an additional field for a counter code Zx.

In the following, the functioning method of the first exemplary embodiment shown in Figure 1 is explained in greater detail. A corresponding identifier K1, ... Kx, ... Kn is stored in base device BG for each remote control F1, ... Fx, ... Fn. Because of this, base device BG is able to clearly identify each individual remote control Fx or each remote-control group Fx - if, for example, a plurality of remote controls Fx are allocated to one identifier Kx. These identifiers K1, ... Kx, ... Kn can be the corresponding memory locations, i.e., can be recognized on the basis of the memory location. In the challenge/response process, the base device transmits challenge Cx to remote control Fx clearly allocated by identifier Kx. A random-sequence generator generates this challenge Cx. Computer 16 stores transmitted challenge Cx in a memory location addressed via identifier Kx. Remote-control computer 20 stores the challenge Cx last transmitted by base device BG in a memory.

The user starts the unidirectional communication of remote control Fx with base device BG by actuating operating control element 24, step 101. Using information specific for the special remote control Fx, remote-control computer 20 combines challenge Cx, stored in the memory, with an algorithm, from which response Rx is formed. For example, a part of identifier Kx, a manufacturing code permanently stored in remote control Fx, is used as information specific to the remote control. However, it is essential that this encryption, i.e., algorithm and information specific to the remote control, of challenge Cx be known and stored for each remote control Fx in base device BG, as well. Code word CWx contains identifier Kx and response Rx, if desired, appropriate wake-up and action commands. Transmitter 22 sends code word CWx to base device BG, step 103. Computer 16 filters identifier Kx out from received code word CWx. Computer 16 selects the challenge Cx, addressed by this identifier Fx, and encryption, which were also used to ascertain response Rx in remote control Fx. Computer 16 calculates required response Sx from challenge Cx, stored in base device BG, from the algorithm and from the information specific to the remote

control, thus from the encryption, step 105. Received response Rx and calculated required response Sx are compared in base device BG, step 107. If they agree, computer 16 gives a corresponding enabling signal, step 109. Otherwise, query 111, as to whether the number of failed opening attempts M has already exceeded a specifiable limiting value G, follows. If this is the case, no further opening attempt is permitted, step 113. In addition, challenge Cx stored in base device BG is erased. Thus, an access authorization can only be achieved by a successful run-through of the bidirectional challenge/response procedure, but not with the unidirectional protocol described. If the number of failed opening attempts M has not yet exceeded limiting value G, number M is incremented, step 115. Following this is step 105; the further procedure takes its course as already described.

The steps from 111 on increase the security of the unidirectional data transmission, but are not absolutely necessary.

The second exemplary embodiment, described in the following, relates to Figures 3 and 4. As already explained for the first exemplary embodiment, challenge Cx is stored in remote control Fx. A counter code Zx, which is incremented in response to actuation of the operating control element 24, is stored in remote control Fx. For each remote control Fx, the last transmitted counter code Zx is stored as reference code RZ1, ... RZx, ... RZn in base device BG. After the start has been triggered by actuating operating control element 24, step 121, in conformity with the first exemplary embodiment, response Rx is calculated. Counter code Zx is increased by one. In addition to response Rx and identifier Kx, counter code Zx is contained in encrypted form in code word CWx. Transmitter 22 sends code word CWx to transmitter/receiver 12, step 123. Computer 16 in turn filters identifier Kx out from received code word CWx, reads out reference code RZx belonging to remote control Fx on the basis of this identifier, step 125. Counter code Zx is subsequently compared to reference code RZx, step 127. Since the counter code Zx last transmitted is stored as reference code RZx in base device BG, given a proper actuation of remote control Fx, counter code Zx and reference code RZx deviate from one another. However, if they agree, is broken off, step 129. An access is not authorized. Otherwise, as already for the first exemplary embodiment, base device BG ascertains required response Sx,

step 131. If response Rx and required response Sx do not agree, step 133, then is broken off, step 135. Otherwise the authorization is given for initiating an opening operation, step 137.

As an alternative second exemplary embodiment, counter code Zx is encrypted in remote control Fx. To ascertain reference code RZx, this encryption must be stored, addressed, in base device BG. It is only important for counter code Zx that it change with each actuation of remote control Fx; whether by a counter function or another algorithm is not important.

The two exemplary embodiments can also be combined to the effect that, for example, in the sequence according to Figure 4, the query according to step 111 is carried out. In this manner, security can be further increased vis-à-vis unauthorized opening attempts.

The challenge/response procedure, not explained more precisely, is preferably carried out at low frequency at short distance of the space to be entered, e.g., a motor vehicle. On the other hand, transmitter 22 transmits a higher-frequency signal which permits a greater transmission range. A receiver in the higher-frequency range is not to be provided for remote control Fx. The algorithm for encrypting challenge Cx in order to obtain response Rx can preferably be realized so simply that it too can be implemented in a microcontroller.

## Patent Claims

1. A system for controlling access authorization,
  - having a base device (BG) which receives a code word (CWx) that contains a response (Rx) which a computer (16) compares to a required response (Sx), an access being authorized if the response (Rx) and the required response (Sx) agree;
  - having at least one remote control (F1, ... Fx, ... Fn) which transmits the code word (CWx),  
characterized in that a challenge (Cx) transmitted by the base device (BG) is stored in the remote control (F1, ... Fx, ... Fn) for generating the code word (CWx).
2. The system as recited in Claim 1,  
characterized in that the required response (Sx) is formed as a function of an identifier (K1, ... Kx, ... Kn) stored in the remote control (F1, ... Fx, ... Fn) and contained in the code word (CWx).
3. The system as recited in one of the preceding claims,  
characterized in that the challenge (Cx) is stored in the base device (BG).
4. The system as recited in one of the preceding claims,  
characterized in that the challenge (Cx) stored in the base device (BG) is erased when the number of failed agreements of the response (Rx) and the required response (Sx) exceeds a specifiable limiting value (G).
5. The system as recited in one of the preceding claims,  
characterized in that the code word (CWx) contains a counter code (Zx) which the base device (BG) compares to a reference code (RZx).
6. The system as recited in one of the preceding claims,  
characterized in that the counter code (Zx) is changed in response to actuation of an operating control element (24) of the remote control (F, ... Fx, ... Fn).
7. The system as recited in one of the preceding claims,

characterized in that a transmitted counter code ( $Z_x$ ) is used as the reference code ( $RZ_x$ ).

8. The system as recited in one of the preceding claims, characterized in that the counter code ( $Z_x$ ) is contained in encrypted form in the code word ( $CW_x$ ).

9. The system as recited in one of the preceding claims, characterized in that the code word ( $CW_x$ ) is transmitted at high frequency and the challenge ( $C_x$ ) is transmitted at low frequency.

09581459.072700

## Abstract

A system is proposed for controlling access authorization. It includes a base device (BG) which receives a code word (CWx) that contains a response (Rx). A computer (16) compares the response (Rx) to a required response (Sx). An access is authorized if the response (Rx) and the required response (Sx) agree. A remote control ((F1, ... Fx, ... Fn) transmits the code word (CWx). The system has the distinction that a challenge (Cx) transmitted by the base device (BG) is stored in the remote control (F1, ... Fx, ... Fn) for generating the code word (CWx).

002270.65412560



Fig. 1

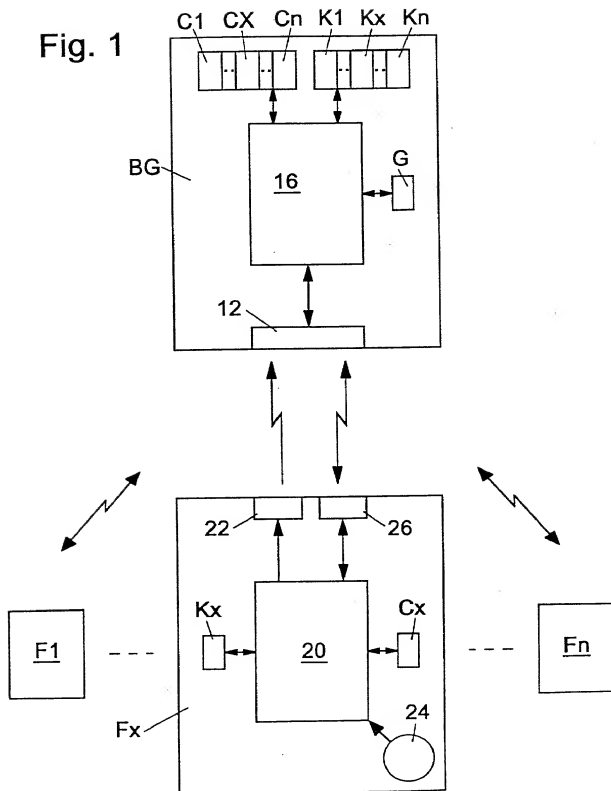


Fig. 2

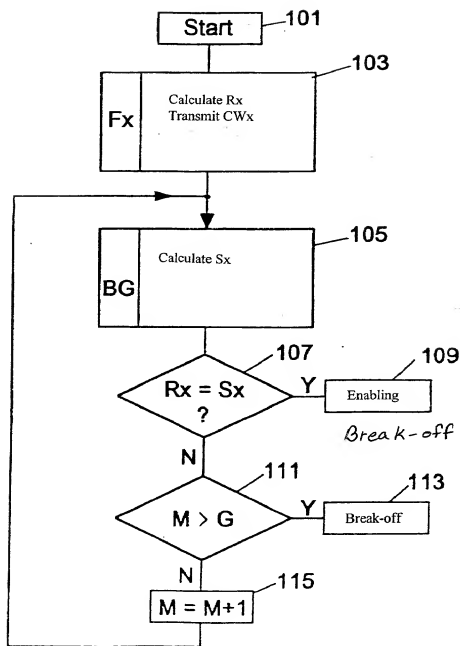


Fig. 3

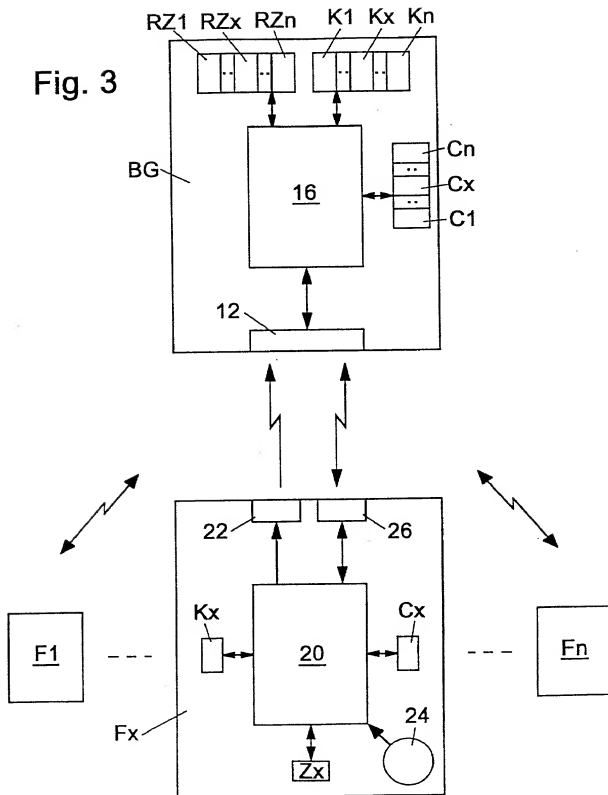
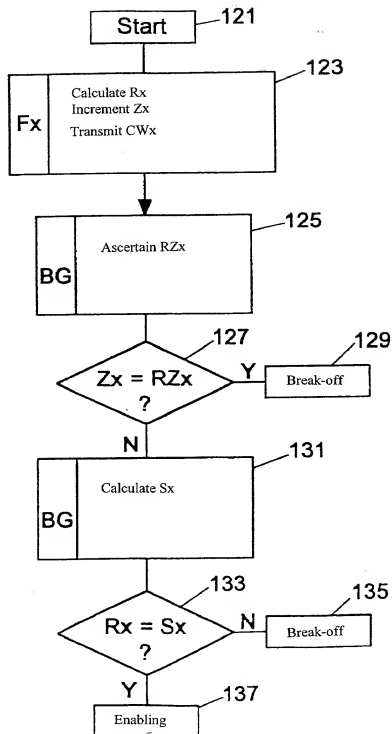


Fig. 4



PATENT  
10191/1452IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : SCHMITZ  
International Application No. : PCT/DE98/03431  
International Filing Date : 20 November 1998  
U.S. Serial No. : 09/581,459  
For : **SYSTEM FOR CONTROLLING ACCESS  
AUTHORIZATION**

Assistant Commissioner  
for Patents  
Box PCT  
Washington, D.C. 20231  
Attention: DO/EO/US

**RESPONSE TO MISSING REQUIREMENTS  
UNDER 35 U.S.C. 371**

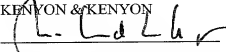
S I R :

In response to the Notification of Missing Requirements Under 35 U.S.C. 371 in the United States Designated/Elected Office (DO/EO/US) (mailed June 30, 2000), Applicants submit herewith a fully executed Declaration, in order to complete the filing requirements for the U.S. national phase of the above-identified PCT application. The application filed in the Patent Office is the application which the inventors executed by signing the Declaration and Power of Attorney. A copy of the Notification of Missing Requirements is also enclosed.

The Office is authorized to charge the \$130.00 fee to cover the surcharge for late filing of the Declaration and any additional fees to Deposit Account No. **11-0600**.

Respectfully submitted,

KENYON &amp; KENYON

  
Richard L. Mayer, Reg. No. 22,490  
One Broadway  
New York, NY 10004  
Tel: (212) 425-7200  
Fax: (212) 425-5288

Date:

7/27/00

EXPRESS MAIL: EL594604823US

299610

09581459-072700

**PRIOR FOREIGN APPLICATION(S)**

| Number       | Country<br>Filed        | Day/Month/Year   | Priority Claimed<br>Under 35 USC 119 |
|--------------|-------------------------|------------------|--------------------------------------|
| 197 55 092.4 | Fed. Rep. of<br>Germany | 11 December 1997 | Yes                                  |

2. And I hereby appoint Richard L. Mayer (Reg. No. 22,490) and Gerard A. Messina (Reg. No. 35,952) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON  
One Broadway  
New York, New York 10004

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: Stephan SCHMITZ

Inventor's Signature: Stephan Schmitz

Date: 12.7.2000

Residence: Seyfferstr. 53  
70197 Stuttgart DEU  
Federal Republic of Germany

*Thomas Dreimann*

ZEUGE

*Thomas Dreimann*

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.

2 - 00

Inventor:

Hans-Joerg MATHONY

Inventor's Signature: \_\_\_\_\_

*Math*

Date: \_\_\_\_\_

4.7.00

Residence:

Schorndorfer Weg 32

71732 Tamm-Hohenstange ~~DEX~~

Federal Republic of Germany

*U. Beutnagel-Buchner*

**ZEUGE**

**UWE BEUTNAGEL-BUCHNER**

Citizenship:

Federal Republic of Germany

Post Office Address: Same as above.

002240.65418560

289302



**DECLARATION AND POWER OF ATTORNEY**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **SYSTEM FOR CONTROLLING ACCESS AUTHORIZATION**, the specification of which was filed as International Application No. PCT/DE98/03431 on November 20, 1998.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

26302699756

EL 594604823US

09581459.072700